Vysoká škola báňská – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Absolvování individuální odborné praxe

Individual Professional Practice in the Company

2018

Tadeáš Janík

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Zadání bakalářské práce

Student: **Tadeáš Janík**

Studijní program: B2647 Informační a komunikační technologie

Studijní obor: 2601R013 Telekomunikační technika

Téma: Absolvování individuální odborné praxe
Individual Professional Practice in the Company

Jazyk vypracování: čeština

Zásady pro vypracování:

1. Student vykoná individuální praxi ve firmě: Audionika s.r.o.
2. Struktura závěrečné zprávy:
a. Popis odborného zaměření firmy, u které student vykonal odbornou praxi a popis pracovního zařazení studenta.
b. Seznam úkolů zadaných studentovi v průběhu odborné praxe s vyjádřením jejich časové náročnosti.
c. Zvolený postup řešení zadaných úkolů.
d. Teoretické a praktické znalosti a dovednosti získané v průběhu studia uplatněné studentem v průběhu odborné praxe.
e. Znalosti či dovednosti scházející studentovi v průběhu odborné praxe.
f. Dosažené výsledky v průběhu odborné praxe a její celkové zhodnocení.

Seznam doporučené odborné literatury:

Podle pokynů konzultanta, který vedl odbornou praxi studenta

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **Ing. Zdeňka Chmelíková, Ph.D.**

Konzultant bakalářské práce: Ing. Jan Odstrčilík, Ph.D.

Datum zadání: 01.09.2017
Datum odevzdání: 30.04.2018

VYSOKÁ ŠKOLA BÁŇSKÁ-TECHNICKÁ UNIVERZITA Fakulta elektrotechniky a informatiky ID16 OSTRAVA

doc. Ing. Miroslav Vozňák, Ph.D.
vedoucí katedry

prof. Ing. Pavel Brandštetter, CSc.
děkan fakulty

Prohlášení studenta

Prohlašuji, že jsem tuto bakalářskou/diplomovou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě dne: *29.dubna 2018*

.....
podpis studenta

Rád bych poděkoval panu Ing. Janu Odstrčilíkovi Ph.D. a panu Ing. Martinovi Odstrčilíkovi za odbornou pomoc a konzultaci při vytváření této bakalářské práce.

Prohlášení zástupce spolupracující právnické nebo fyzické osoby

„Souhlasím se zveřejněním této bakalářské práce dle požadavků čl. 26, odst. 9 Studijního a zkušebního řádu pro studium v bakalářských/magisterských programech VŠB-TU Ostrava."

Dne 29. dubna 2018

.....
podpis zástupce

AudioNIKA...
Jasenice 108, 756 41 Lešná
Tel.1: 731 157 590, Tel.2: 731 157 59
www.audionika.cz, mail@audionika.cz
IČO: 25359827, DIČ: CZ25359827

Abstrakt

Tato bakalářská práce představuje popis úkolů a jejich řešení, které jsem absolvoval během odborné praxe ve firmě AudioNIKA s.r.o. V práci je popsáno odborné zaměření firmy, zadané úkoly, jejich řešení a technologie, které byly při daných úkolech použity.

Síťová infrastruktura firmy je zastaralá a zadáním bylo jí vylepšit. Vize byla porovnat původní a novou síť a přidat několik vylepšení, jako je vzdálený přístup k síti nebo možnost vzdáleného zálohovaní dat na síťový disk.

Na konci práce budou zhodnoceny získané zkušenosti, celkové shrnutí a přínos úkolů, které jsem provedl.

Klíčová slova

Cloud; firma; GDPR; kapacita; LAN; NAS; OpenVPN; přenosová rychlost; router; síť; úložiště; Wi-Fi;

Abstract

This bachelor thesis presents a description of the tasks and their solution, which I passed and learned during my professional experience in AudioNIKA s.r.o. The thesis describes the professional orientation of the company, the assigned tasks, their solutions and technologies that were used in the given tasks.

The company's network infrastructure is very outdated and I have the task of upgrading. The vision is to compare the original and new network infrastructure and add some improvements such as remote network access or remote data backup on the device.

At the end of the thesis I evaluate the gained experience and the overal summary and contribution of the tasks I have worked on.

Key words

baud rate; capacity; Cloud; company, GDPR; LAN; NAS; network; router; storage; OpenVPN; Wi-Fi;

Seznam použitých zkratek

Zkratka	Význam
AP	Access Point
DHCP	Dynamic Host Configuration Protocol
DPO	Data Protection Office
GDPR	General Data Protection Regulation
GUI	Graphical User Interface
HDD	Hard Disk Drive
IP	Internet Protocol
KRACK	Key Reinstallation Attacks
LAN	Local Area Network
NAS	Network Attached Storage
OS	Operating System
QR	Quick Response
RAID	Redundant array of Independent Disks
SCP	Secure Copy Protocol
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
USB	Universal Series Bus
UTP	Unshielded Twisted Pair
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wireless Area Network
WPA	Wi-Fi Protected Access
Wi-Fi	Wireless Fidelity

Seznam ilustrací

Obsah

Úvod

Bakalářská odborná praxe poskytuje možnost studentům nabýt znalosti a zkušenosti formou praxe ve firmě. Tato možnost mě velmi zaujala, protože jsem se dostal do spolupráce s firmou AudioNIKA s.r.o. Firma potřebovala vylepšit několik věcí, které se týkali informatiky/telekomunikací. Z toho důvodu jsem si praxi vybral a snažil se splnit požadavky firmy a zároveň nabýt znalosti, které by mě posunuly v mém vzdělání o krok dál. Tématem této bakalářské práce je popis průběhu plnění zadaných úkolů ve společnosti AudioNIKA s.r.o.

Práce je rozdělena do 3 hlavních kapitol. Každá kapitola má několik jednotlivých dílčích témat, kterými jsem se zabýval.

První kapitola se zabývá navýšením přenosové kapacity, propustnosti a dostupnosti firemní sítě. Bylo potřeba zrychlit přístup ke sdíleným zdrojům, navýšit stabilitu a dostupnost drátového i bezdrátového spojení. Dále umožnit přístup k internetu návštěvníkům firmy bez možnosti přístupu do interní sítě a síť řádně zabezpečit. Následně konfiguraci sítě zdokumentovat.

Druhá kapitola řeší nastavení firemní VPN, která klade důraz na zabezpečení před propustností a bude dostupná pro všechny platformy operačních systémů. Přístup bude řešen pomocí hesla nebo privátních klíčů. Konfigurace musí být maximálně jednoduchá, například pomocí instalačního balíčku pro danou platformu.

V třetí a zároveň poslední kapitole bylo cílem realizovat privátní cloudové úložiště, které by současný a neefektivní způsob zálohovaní dat zjednodušilo. Úložiště musí být bezpečné, každý zaměstnanec musí mít nastaven svou osobní složku na zálohu dat s nastavením kvóty o určitém objemu dat a přístup k zálohovaným souborům musí být umožněn jak z interní sítě, tak přes zřízené VPN. Autentizace je řešena pomocí uživatelského jména a hesla, které již má zaměstnanec přiděleno.

1 Odborné zaměření firmy AudioNIKA s.r.o.

1.1 Odborné zaměření firmy

Společnost AudioNIKA s.r.o. byla založena v roce 1996 s cílem poskytovat sluchově postiženým lidem komplexní služby k jejich plné spokojenosti. Ale nejen jim, také ušním lékařům či foniatrům, a také speciálním pedagogům i logopedům.

AudioNIKA s.r.o. spolupracuje se světově známými firmami v tomto segmentu trhu a tuto spolupráci se snaží postupně dále rozvíjet. Od roku 2003 zahájila spolupráci s firmou MED-EL, která je rakouským výrobcem kochleárních implantátů.

Společnosti AudioNIKA s.r.o. v současné době působí v těchto hlavních audiologických oborech a poskytuje následující služby:

- Dovoz, distribuce a servis kochleárních, středoušních a kostních implantátů firmy MED-EL.
- Dovoz, prodej a servis sluchadel SONIC, nastavování většiny značek sluchadel pomocí výpočetní techniky.
- Dovoz, prodej a servis diagnostických přístrojů pro ORL od firmy Natus (Otometrics).
- Dovoz a prodej baterii do sluchadel a implantátů firmy iCellTech.
- Dovoz, prodej a servis bezdrátových naslouchacích souprav a bytových signalizací pro sluchově postižené od firmy Phonic Ear.
- Jako autorizovaný distributor prodej a servis audiologických naslouchacích pomůcek a ozvučení veřejných prostor (kina, divadla, kostely, sály...) pro potřeby sluchově postižených značky Sennheiser.
- Distribuci produktů pro diagnostiku a nápravu řeči.

1.2 Popis pracovního zařazení

Ve firmě jsem byl pověřen jako IT podpora a technik sluchadel firmy SONIC a dalších audiologických přístrojů. Poskytuji sluchově postiženým lidem technické poradenství při korekci jejich sluchové vady vhodnou kompenzační pomůckou na základě vyšetření odborným lékařem. Zákazníci/pacienti se taktéž mohou na firmu obrátit se servisem kompenzačních pomůcek, případným doladěním nebo zaškolením přístrojů. Ve firmě působím také jako IT podpora, mám na starost počítačovou síť firmy, její zařízení, webové stránky, e-shop a další IT služby.

2 Zadané úkoly při vykonávání odborné praxe

2.1 Navýšení přenosové kapacity, propustnosti a dostupnosti firemní sítě

Současná podniková síť již nesplňuje požadavky na spolehlivost, dostupnost, rychlost a rozšiřitelnost. Vedením a pracovníky firmy byly stanoveny požadavky na současnou síťovou infrastrukturu:

- Zrychlení přístupu ke sdíleným zdrojům, zejména kopírování obsahu ze, respektive do sdílených adresářů.
- Navýšení stability a dostupnosti drátového i bezdrátového spojení v odlehlejších nebo stíněných částí firmy.
- Zapojení dalších zařízení (síťová tiskárna, firemní server, zařízení v rámci serveru nebo realizaci zakázky).
- Umožnění přístupu k internetu návštěvníkům firmy bez možnosti vstupu do interní sítě.
- Zabezpečení současné sítě proti aktuálním zranitelnostem.
- Nastavení pravidel podnikové sítě v souladu s GDPR.

2.2 Firemní VPN

Pracovníci firmy potřebují přistupovat ke sdíleným zdrojům ze vzdálených lokací, např. při realizaci zakázek, v průběhu výjezdu k zákazníkům a v neposlední řadě z provozoven a detašovaných pracovišť. Tento problém by se měl řešit pomocí firemní VPN (Virtual Private Network), která by měla splňovat následující požadavky:

- Připojení a zabezpečení i za cenu nižší propustnosti sítě.
- Dostupnost připojení pro uživatele operačních platforem – Windows, iOS a Android.
- Autentizace uživatelů pomocí hesla nebo privátních klíčů.
- Maximálně jednoduchá konfigurace připojení, např. pomocí instalačního balíčku pro danou platformu.
- Nastavení pravidel v souladu s GDPR.

2.3 Privátní cloudové úložiště s automatickým zálohováním dat

V současnosti si zaměstnanci firmy vyměňují data, např. manuály, instalační soubory dodávaných softwarů a jiné elektronické dokumenty a data pomocí fyzických zařízení (USB), e-mailů nebo veřejných služeb ke sdílení dat. Z důvodu citlivosti některých dat je žádoucí realizovat privátní cloudové úložiště, které by současný způsob výměny dat nahradilo, zefektivnilo a zjednodušilo. Firma si od zavedení služby slibuje:

- Bezpečné a spolehlivé úložiště pro sdílení dat mezi zaměstnanci s historií změn a notifikacemi v případě změny obsahu.
- Zřízení privátní složky pro každého zaměstnance s nastavením kvóty na objem dat.
- Automatické zálohování zvolených adresářů z firemních zařízení zaměstnanců – notebooky, PC, telefony.
- Dostupnost cloudových služeb z interní sítě vzdáleně přes VPN.
- Autentizace pomocí uživatelského jména a hesla, které již zaměstnanec má přiděleno.
- Nastavení pravidel v souladu s GDPR.

3 Postup řešení zadaných úkolů

3.1 Navýšení přenosové kapacity, propustnosti a dostupnosti firemní sítě

3.1.1 Zrychlení přístupu ke sdíleným zdrojům, navýšení stability a dostupnosti drátového i bezdrátového spojení

Zajištění stabilní internetové sítě se bude realizovat ve firmě, jejíž budova má 3 podlaží, sklad a parkovací plochu. Sklad není součástí budovy firmy a je nutné ho také pokrýt. Parkoviště a okolí zhruba 5 metrů musí mít připojení k návštěvnické Wi-Fi (2,4 GHz) i za cenu slabšího signálu. Primárním cílem je pokrýt všechny 3 patra budovy. V původním zapojení byly 2 routery. Jeden hlavní v prvním patře, který přestává být dostačující z důvodu malého počtu LAN (Local Area Network) portů, jen 2,4 GHz sítě a pouze 100Mbit LAN přenosu. Vzhledem k popsanému nedostatečnému síťovému pokrytí je nutné realizovat určitá vylepšení. Signál nedosahoval do okolí vzdálenějšího, než je sama budova. Největší problém byl v přízemí, ve kterém byl signál takřka nulový. Druhý router je ve druhém patře, který funguje jako AP a rozšiřuje danou síť.

Vizí bylo vytvořit dvě sítě, které budou rozlišovat připojené uživatele, tedy síť pro pracovníky firmy a síť pro návštěvníky. V každé síti budou nastavena taková pravidla, aby se ke zdrojům dostaly jen ty osoby, které mají přístup umožněn.

Rozhodl jsem se tedy vybrat router s vlastním operačním systémem, který bude mít otevřenou Linuxovou distribuci a bude možné ho spravovat téměř jako Linuxový server. Zároveň je také třeba zavést Gigabitový provoz, protože firma do teď fungovala pouze na 100Mbitové síti. Z tohoto důvodu byl vybrán server NAS (Network Attached Storage), který bude sloužit pro zálohování a vzdálené připojení k souborům přes vytvořenou VPN síť. Záloha bude probíhat mnohem rychleji na Gigabitové síti.

Po zvážení byl vybrán router Turris Omnia 1 GB. Tento router zaujal prakticky ihned a ve výsledném přednesení vedení firmy jsem jej jasně prosazoval před ostatními routery.

Router Turris Omnia má nejvíce pokročilých funkcí. Router má vlastní operační systém a možnost dokoupení libovolných modulů pro různé modifikace.

Velkou výhodou routeru jsou tzv. „Honeypoty“. Ty vytvářejí falešné služby na různých portech a simulují napadnutelný systém. Router je možno nastavit tak, aby se určitý provoz přesměroval do honeypotu a potom můžeme sledovat, o co se útočník pokoušel, protože se všechny jeho akce zaznamenávají. Honeypot tedy ukazuje síť jako lehce napadnutelnou a zároveň využívá těchto útoků pro vylepšení ochrany. Výhoda je hlavně v tom, že honeypoty jsou u poskytovatele, ne na místním zařízení, tím pádem ani nezatěžují provoz. [2]

Předností routeru je také rozšiřitelnost, kdy je možné dokoupit několik doplňujících modulů a přidat tak na příklad DVB-T tuner a sdílet s počítači v síti televizní vysílání nebo přidat zvukovou kartu a využít jako internetové rádio. Nejvíce fascinující z doplňkových modulů byla možnost dokoupení webové kamery, která udělá z routeru jednoduchý alarm proti zlodějům, který bude sám e-mailem zasílat fotografie.

Router má výhodu operačního systému založeného na OpenWrt, což je linuxová distribuce. K dispozici router poskytuje 3 gigabitové ethernetové linky, což bylo bráno v potaz, aby nemusel k routeru být dokupován switch a bylo možné kabely využít i do jiných pater, kde už signál není dostačující.

Turris Omnia (Obr.-3.1) disponuje dvěma uživatelskými prostředími. Prvním je „základní“ rozhraní FORIS, které zvládne i dosti laický uživatel. Druhým „pokročilým“ rozhraním je LuCI, které je naopak určeno znalým a zkušeným uživatelům. Využívá se i konfigurace přes příkazový řádek.

Obrázek 3.1 *Router Turris Omnia [1]*

3.1.2 **Zapojení routeru do sítě a nastavení**

Po zapojení routeru naběhl průvodce, který v jednotlivých krocích asistoval při nastavení. Velice nápomocná může být zvláště po nezkušené uživatele kontrola zadaných hodnot, která při vložení např. IP adresy okamžitě kontroluje, zda byla hodnota zadaná správně a zda bude připojení fungovat.

Při konfiguraci sítě bylo nastaveno jako první Wi-Fi heslo. Poté bylo třeba nastavit WAN (wireless area network) síť, kde IPv4 adresa je konfigurovaná staticky podle údajů přidělených internetovým poskytovatelem. Bylo potřeba zadat MAC (Media Access Control) adresu, která byla totožná se stávající, kterou už měl poskytovatel z předchozího routeru uloženou v jejich databázi. K ověření slouží část průvodce *Connectivity test*, která prověří, zda jsou nastavení WAN správná. Jako DNS (Domain Name System) byly nastaveny servery poskytovatele internetu, které jsou stabilní a výkonné.

V LAN části průvodce byla nastavena IP adresa routeru. Potom jsem přešel na nastavení DHCP (Dynamic Host Configuration Protocol). Ta byla důležitá z důvodu přidělování IP adres uživatelům. Bylo nastaveno 150 možných IP adres, které budou přidělovány návštěvníkům a zaměstnancům firmy.

Konfigurována byla také možnost *Notification settings*, která umožňuje zasílat informace o routeru, např. o požadovaném restartu zařízení instalaci aktualizací nebo potenciálních problémech. Tyto informace zasílá jako e-mailové zprávy. Pro zasílání zpráv bylo nutné zadat e-mailovou adresu. Bylo však zjištěno, že není doporučeno používat vlastní e-mail, neboť heslo e-mailu se ukládá v konfiguračních souborech v čitelné podobě. Z toho důvodu byl vytvořen e-mailový účet, který bude sloužit pouze pro notifikace z routeru.

Pro Wi-Fi připojení jsem nastavil jak 2,4 GHz tak i 5 GHz síť. 5 GHz síť je v patře s konferenčními místnostmi silná a bude vhodná jak pro zálohování dat, tak pro větší propustnost. 5 GHz síť však bylo možné zprovoznit pouze v případě, že byla aktivovaná síť 2,4 GHz. Antény na routeru jsou propojené a jedna nedokáže bez druhé pracovat. V tomto případě 5 GHz síť nedokáže pracovat bez 2,4 GHz.

Na routeru se automaticky instalují aktualizace bez přerušení provozu. Výjimkou je potom případná aktualizace jádra OS router. Zde byl nastaven plán případné aktualizace na noční provoz.

3.1.3 Testování rychlostí z/do sdílených adresářů

Pro porovnání přenosové rychlosti původního 100-Mbitového routeru a nového routeru Turris Omnia, byl zapojen napřed původní, starý router a připojené přes něj 2 koncové zařízení (notebooky). Po proběhnutí měření byla odpojena obě zařízení od LAN sítě a připojena k Wi-Fi síti (starý router uměl pouze 2,4 GHz síť), kde bylo nutné provést totéž. Stejný proces byl proveden s novým routerem, jen byla navíc naměřena i propustnost 5 GHz sítě.

Měření se provádělo pomocí programu Iperf, který je určen pro měření a ladění výkonu sítě. Iperf má funkci klienta a serveru, tudíž může vytvářet datové toky pro měření propustnosti mezi oběma konci v jednom nebo obou směrech. Typický výstup obsahuje časově označenou zprávu o množství přenesených dat a naměřené propustnosti. Tyto výstupy jsou zde nyní popsány a slouží k porovnání naměřených hodnot starého a nového routeru a poté vyneseny do grafu.

Nejdřív byly propojeny obě zařízení přes router síťovým UTP kabelem a vyzkoušen ping pro zjištění, zda se počítače navzájem vidí. Potom v programu Iperf bylo jedno zařízení nastaveno jako server a druhé jako klient. Následně byla zvolena velikost souboru, jaká se bude posílat a zahájena výměna (Obr. 3.2). Velikost souboru byla zvolena na 600 MB.

Starý router - TP-LINK TL-WR841N				
Čas	LAN - 100Mbit		2,4 GHz wlan 802.11g-100Mbit	
	Poslané data [MB]	Rychlost [Mbits/sec]	Poslané data [MB]	Rychlost [Mbits/sec]
0.00-1.00	11.5	96.4	2.12	17.08
1.00-2.00	11.2	94.4	1.88	15.07
2.00-3.00	11.4	95.4	2.12	17.08
3.00-4.00	11.2	94.4	2.00	16.08
4.00-5.00	11.4	95.4	1.75	14.07
5.00-6.00	11.4	95.5	1.75	14.07
6.00-7.00	11.2	94.4	1.75	14.07
7.00-8.00	11.2	94.3	2.25	18.09
8.00-9.00	11.4	95.3	2.00	16.08
9.00-10.00	11.4	95.4	2.00	16.08
10.00-11.00	11.2	94.4	2.12	17.08
11.00-12.00	11.4	95.6	1.88	15.07
12.00-13.00	11.2	94.3	2.12	17.08
13.00-14.00	11.4	95.4	2.12	17.08
14.00-15.00	11.2	94.4	2.12	17.08
15.00-16.00	11.4	95.4	2.12	17.09
16.00-17.00	11.2	94.4	1.75	14.07

Obrázek 3.2 *Přenos souboru na starém routeru*

Po naměření přenosových rychlostí LAN a Wi-Fi na starém routeru byla připojena koncová zařízení k novému routeru Turris Omnia a proveden přenos souboru o stejné velikosti po LAN a Wi-Fi síti (Obr. 3.3).

Nový router - Turris Omnia 1GB						
Čas	LAN - 1Gbit		2,4 GHz wlan 802.11ac -1Gbit		5 GHz wlan 802.11ac -1Gbit	
	Poslané data [MB]	Rychlost [Mbits/sec]	Poslané data [MB]	Rychlost [Mbits/sec]	Poslané data [MB]	Rychlost [Mbits/sec]
0.00-1.00	81,5	683	2.12	17.08	14.8	124
1.00-2.00	51,4	683	2.00	16.07	14.9	125
2.00-3.00	84,4	708	1.88	15.08	15.2	128
3.00-4.00	94,6	794	2.00	16.07	14.2	120
4.00-5.00	94,8	795	2.12	17.08	14.6	123
5.00-6.00	84,1	705	2.25	18.08	15.1	127
6.00-7.00	79,2	671	2.12	17.08	14.8	124
7.00-8.00			1.88	15.08	14.8	124
8.00-9.00			2.12	17.08	15.0	126
9.00-10.00			2.12	17.08	14.8	124
10.00-11.00			1.88	15.07	14.6	123
11.00-12.00			2.00	16.08	15.1	127
12.00-13.00			2.12	17.08	15.0	126
13.00-14.00			2.00	16.08	15.2	128
14.00-15.00			2.12	17.08	15.0	126
15.00-16.00			1.88	15.07	15.0	126
16.00-17.00			2.12	17.08	15.0	126

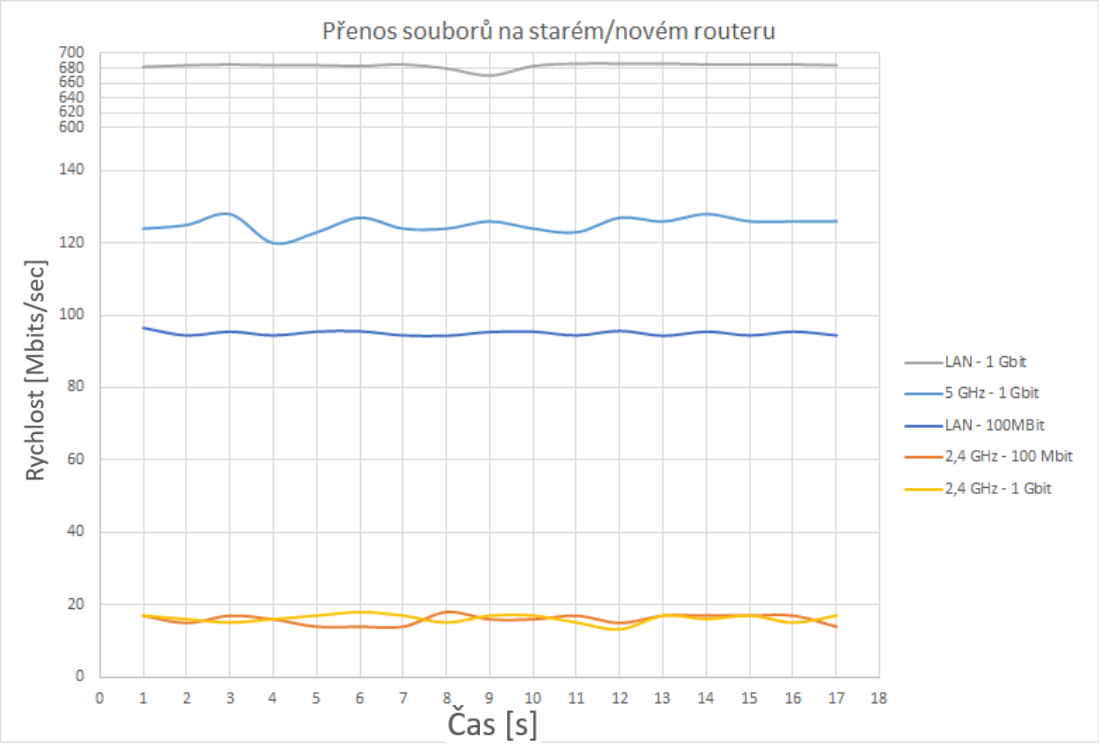
Obrázek 3.3 *Přenos souboru na novém routeru*

Jak můžeme vidět výše, u nového routeru je přenos souboru po 2,4 GHz Wi-Fi síti téměř stejně rychlý (kolem 16 Mbit/s), jako přenos na starém routeru. Připojení a posílání souborů pomocí ethernetového kabelu k LAN síti nového routeru je potom neporovnatelně vyšší (kolem 700 Mbit/s) na novém a kolem 95 Mbit/s na starém). 600MB soubor se poslal za 7 s, na starém routeru trval přenos

17 s. Data firmy se budou zálohovat místo na externí disk přes NAS úložiště a přenos souborů bude tedy znatelně rychlejší.

Stávající router TP-Link neměl 5GHz síť. Ta tedy není s čím porovnatelná, ale pro zajímavost byla také změřena. Zde je přenosová rychlost znatelně vyšší než na 2,4GHz síti (kolem 125 Mbits/s), ale s menším rozsahem. Naměřené rychlosti přes Wi-Fi síť mohou mít drobné odchylky z toho důvodu, že na starém routeru byla přenosová rychlost měřena na zařízeních v naprosté blízkosti, když to při přenosu po novém routeru byla zařízení v cca 6 m vzdálenosti.

Následující graf (Obr. 3.4). znázorňuje všechny viditelné přenosové rychlosti jak na původním, tak na novém routeru.



Obrázek 3.4 *Graf přenosových rychlostí na starém a na novém routeru*

3.1.4 Navýšení stability a dostupnosti drátového i bezdrátového spojení v odlehlejších nebo stíněných částí firmy

Stabilita spojení, především bezdrátového, byla při původním provedení slabá a jedním z požadavků firmy při inovaci bylo se ujistit, že stabilita drátového i bezdrátového spojení bude kvalitní i v odlehlejších nebo stíněných částí firmy.

Hlavním úkolem bylo umístit oba routery do takové pozice, aby signál pokryl celou budovu (3 patra) a zároveň parkoviště se skladem, které jsou v blízkosti budovy. Druhý router bude použit jako AP.

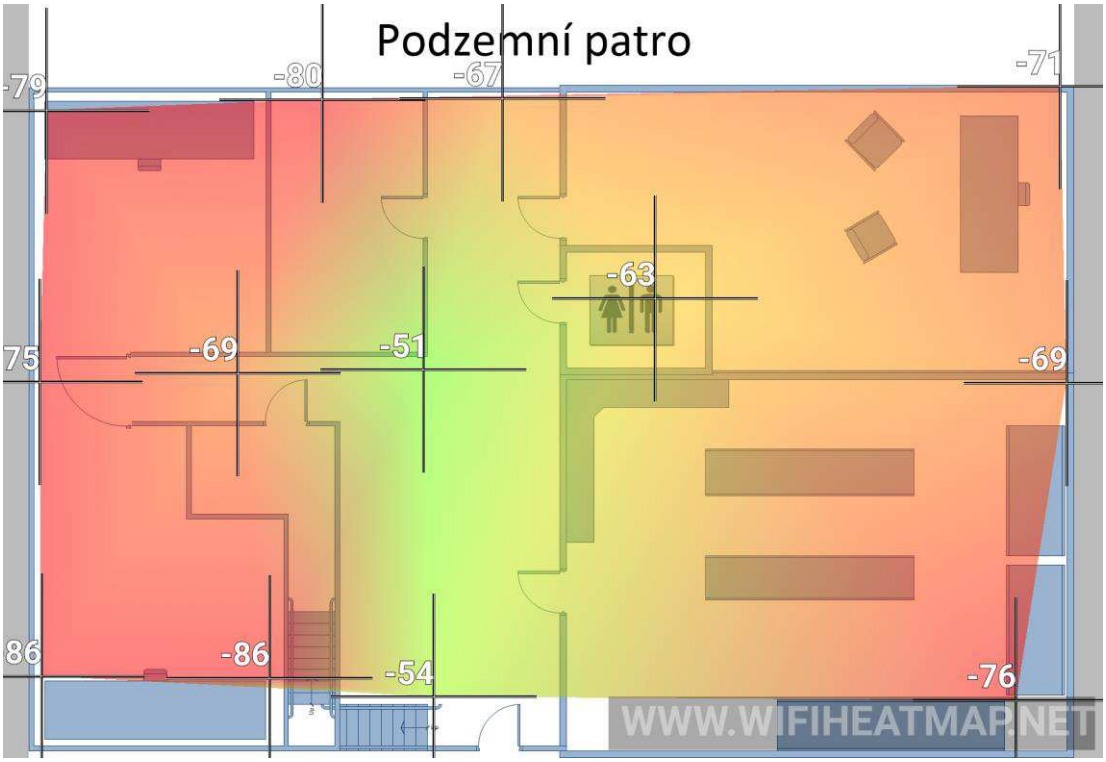
V další fázi byla zmapována budova, okolí a vyměření síly signálů v daných místech. Podle nejlepšího pokrytí bylo nutné umístit router v prvním patře a potom druhý router v patře druhém. Ten bude muset pokrýt signálem i venkovní sklad. Hlavní router Turris Omnia kvůli kabelovému připojení může být pouze v konferenční místnosti v prvním patře (největší místnost v budově) (Obr. 3.5).

Při umístění nového routeru v rohu místnosti, kde je více elektroniky, TV, apod. ale došlo k problému. Při zapojení byla síla signálu nestabilní a slabší, než by měla být. Při podrobnějším zkoumání bylo zjištěno, že na stejném místě je set-top-box, který bránil routeru v šíření signálu, jelikož router byl položen na něm. Po zvážení byl router dle měřených hodnot síly signálu v budově přemístěn do druhého rohu místnosti, ve kterém je více ve středu budovy, a tudíž i pro šíření signálu celou budovou lepší. Signál byl najednou o poznání lepší a problémy ustaly.

V tomto případě byla využita Android aplikace Wi-Fi Analyzer [5], která ukáže všechny Wi-Fi připojení v okolí, kanály a síly signálů. Aplikace zároveň pomůže zjistit, kolik Wi-Fi signálů je v okolí a podle toho budu případně měnit vysílací kanály, aby se signály nerušily [1].

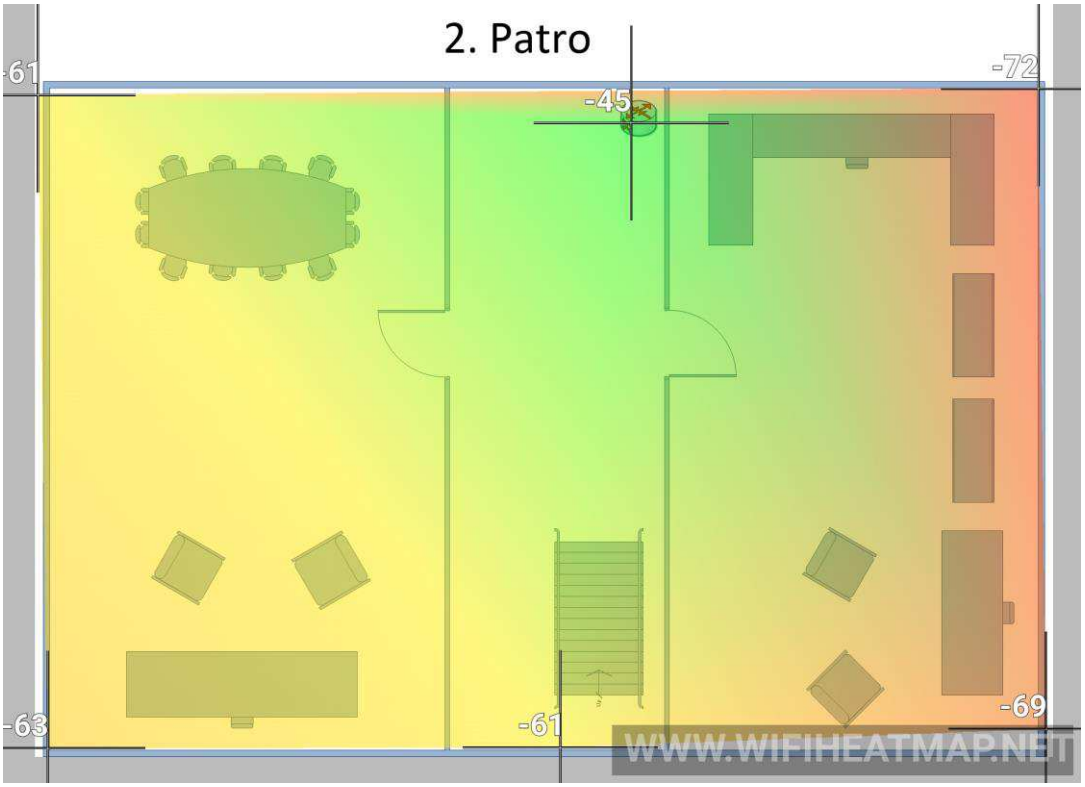
Byla také použita Android aplikace Wifi Heat Map [4], pomocí které byly zmapovány všechny patra, celý pozemek firmy a změřeny síly signálu v různých částech budovy. Konečné umístění má výhodu v tom, že z 90% signál pokrývá budovu (v některých místech však pouze 2,4 GHz) a zároveň nepřesahuje daleko od budovy, pouze v nejbližším okolí, ve kterém je i sklad firmy.

Výsledkem jsou plány celého pozemku firmy (Obr. 3.7), dále podzemního, prvního a druhého patra (Obr. 3.5, 3.6, 3.7), které překrývá heat mapa a data znázorňující sílu signálu. Data jsou uvedena v jednotkách útlumu dBm.

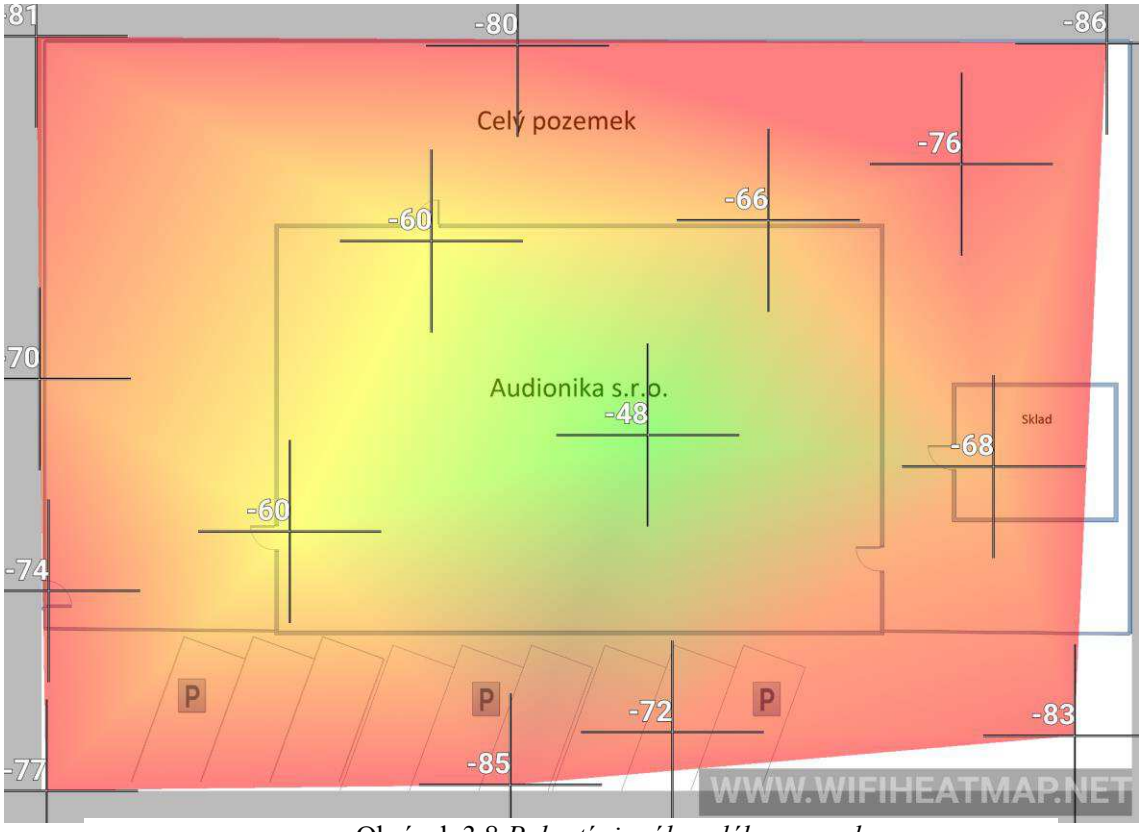


Obrázek 3.5 *Pokrytí signálu podzemního patra*

Obrázek 3.7 *Pokrytí signálu v 1. patře*



Obrázek 3.6 *Pokrytí signálu ve 2. patře*



Obrázek 3.8 *Pokrytí signálu celého pozemku*

3.1.5 **Zapojení dalších zařízení (síťová tiskárna, firemní server, zařízení v rámci serveru nebo realizaci zakázky)**

Nový Wi-Fi router má více výstupů pro zapojení dalších připojení jako například externí tiskárny, servery apod. V případné nouzi bude možné odstranit jeden z LAN kabelů, který je v jedné z kanceláří díky silnějšímu Wi-Fi signálu využíván minimálně. V případě potřeby dalších výstupů by se řešilo individuálně v místě kanceláře pomocí switche.

3.1.6 **Umožnění přístupu k internetu návštěvníkům firmy bez možnosti vstupu do interní sítě**

Uživatelské rozhraní routeru umožňuje zprovoznit dvě stejné Wi-Fi sítě, jednu soukromou a jednu návštěvnickou, tzv. Guest network. Ta povolí Wi-Fi pro hosty, která je oddělena od vnitřní sítě. Zařízení v této síti mohou na internet, ale nemají přístup k ostatním zařízením ani k nastavení routeru. Postačilo zapnout tuto funkci a vytvořit heslo pro návštěvnickou síť. Při aktivování této sítě příjemně překvapila možnost, kde byla volba nastavit propustnost dané návštěvnické sítě. Rychlost bylo možno omezit dle libosti.

Jako návštěvnickou síť bylo možné vytvořit pouze 2,4 GHz síť, 5 GHz nebylo možné povolit. Neočekávané bylo přidělování již zmíněného povoleného počtu IP adres. Nastavení rozsahu, ve kterém bude přidělovat IP adresy, jinak řečeno počet uživatelů, kteří se budou moc k síti připojit, lze nastavit pouze v interní síti. V návštěvnické síti tato možnost chybí, nastavení DHCP se tedy sdílí pro obě sítě a množství připojených uživatelů je tím omezeno na stejný počet, jaký je nastaven v hlavní interní síti.

Uživatelé připojení na návštěvnickou síť se mohou připojit pouze k internetu, ale k žádným jiným zařízením firmy (tiskárny, NAS server atd.). Zároveň je eventualita pro správce sítě vidět všechna připojená zařízení do této sítě, ale zařízení neuvidí nikoho jiného.

Další zajímavostí, která je však v dnešní době běžná, byla situace vytvoření QR (Quick Response) kódu, který umožní po naskenování do mobilního telefonu automatický přístup a přihlášení do Wi-Fi sítě. Jakémukoliv návštěvníkovi by tedy stačilo jen přijít do firmy, naskenovat si QR kód a okamžitě bude připojený k naší síti. Nevýhoda QR kódu je, že nejde nastavit pouze pro „Guest Network“, ale jen pro hlavní firemní síť. V praxi by to znamenalo, že by si kód mohl kdokoliv vyfotit a připojit se.

3.1.7 Zabezpečení současné sítě oproti aktuálním zranitelnostem

Důležité je pro firmu zabezpečení a ochrana dat, která nesmí být zneužitelná. Velkou hrozbou je tak například KRACK (Key Reinstallation Attacks) útok [6]. Při připojení mezi Wi-Fi routerem a koncovým zařízením, tedy počítačem nebo mobilním telefonem útok zneužívá chyby během otevírání zabezpečeného spojení. Router s koncovým zařízením si vyměňuje v několika krocích šifrovací klíče (tzv. handshake) a KRACK díky chybě WPA2 v třetím kroku dokáže tento klíč získat.

V praxi to znamená, že útočník pomocí KRACK útoku může zachytit klíč a síť potom může odposlouchávat. To znamená že po vašem připojení k síti má útočník přehled o vaší aktivitě na internetu a může mít přístup k vašim přihlašovacím údajům a heslům.

Jednou z věcí, jak těmto útokům předejít je mít zaktualizované Wi-Fi ovladače na počítačích a hlavně mít nejnovější aktualizace na routerech. Toto bylo jedním z důvodů, proč byl vybrán router Turris Omnia, protože výrobce routeru jej pravidelně automatizovaně aktualizuje za běhu a není třeba dalších zásahů. Má tedy vždy nejnovější ochranu. Router ASUS RT-N12, který je umístěn ve druhém patře nebyl dlouho aktualizován, a tudíž byla provedena nejnovější aktualizace.

3.1.8 Nastavení pravidel v souvislosti s GDPR

GDPR jsou nařízení o ochraně fyzických osob v souvislosti se zpracováním osobních údajů. Osobními údaji jsou myšleny všechny informace o fyzické osobě, dle kterých lze danou osobu identifikovat. GDPR definuje osobní data jako informace, které se vztahují k jednotlivcům čili subjektům. To mohou být jakákoliv data nebo informace jako jsou například fotografie, email, adresa, bankovní účet a jeho detaily, posty na sociálních sítích, zdravotní informace nebo i web cookies či IP adresa připojení osobního počítače. [7]

Je to tedy poměrně široká definice toho, co může vést k identifikaci jednotlivce.

V praxi tedy bude znamenat zavedení GDPR mnohem více informací při objednávkách na internetu, bude třeba logování času udělení a odebrání souhlasů, potřeba neukládat data nekonečně dlouho, hlásit každý incident narušení bezpečnosti na určitý úřad, být si jistý, že vyžadovaná osobní data jsou skutečně potřebná a že při jakékoliv manipulaci s osobními daty mám od daného subjektu právo. Zákazník musí být seznámen s hodně informacemi před poskytnutím osobních údajů. Bude tedy třeba subjekt seznámit s tím, kdo jsme, proč osobní údaje zpracováváme a jak dlouho je budeme zpracovávat, případně kontakty na správce, zpracovatelé a další.[14]

K jednotlivým bodům vzniknou směrnice, jejichž vypracování ale není předmětem této práce. V této práci je dále v jednotlivých kapitolách zmíněno nastavení pravidel v souvislosti s GDPR. Pro co nejbližší soulad s pravidly GDPR bude v infrastruktuře prováděno následující:

- Pravidelná aktualizace software síťových prvků.
- Pravidelné aktualizace software na koncových zařízeních.
- Pravidelná změna hesla k interní Wi-Fi.
- Důslednost v nevpuštění návštěvníků k síťovým prvkům a přístup pouze k návštěvnické Wi-Fi.

3.2 Firemní VPN

3.2.1 Připojení a zabezpečení i za cenu nižší propustnosti

VPN neboli Virtual Private Network, umožňuje propojení počítačů do zabezpečené soukromé sítě a to i v případě, když se k internetu připojujeme na různých „veřejných“ místech. Díky VPN se vytvoří zašifrovaná cesta neboli tunel, kterým probíhá veškerá komunikace mezi VPN klientem a serverem, pokud není nastaveno jinak. Používá se například pro bezpečné vzdálené připojení do firemní sítě a přístupu k firemním datům.

VPN klient, který je na vašem počítači, nejprve zašifruje data a odešle na daný VPN server, který data rozšifruje a přepošle je dále na cílový server, např. webovou adresu. Stejný postup je potom i v opačném směru. Díky VPN tedy nikdo nevidí vaši skutečnou IP adresu ani weby, které jste během připojení navštívili. Jediné, co je viditelné, je adresa VPN serveru. Hlavním důvodem VPN je tedy ochrana soukromí. [9]

VPN má samozřejmě i nějaké nevýhody. Jako za každou podobnou službu, i za poskytnutí VPN připojení musíme většinou zaplatit. Další nevýhodou je odezva, která se prodlouží, pokud se přes VPN připojíme. Záleží taky na vzdálenosti, která je mezi počítačem, VPN serverem a koncovým server. Čím více vzdálené jsou, tím horší latence. Kvalitní VPN mohou dosahovat rychlostí až kolem 100 Mbps. Samozřejmě záleží také na rychlosti veřejné sítě, ke které jsme připojeni.

3.2.2 Dostupnost připojení pro uživatele všech operačních platforem - Windows, Linux, iOS a Android

Byla zvolena varianta OpenVPN, která se jeví jako nejvhodnější. OpenVPN využívá protokoly SSLv3 / TLSv1 a knihovnu OpenSSL, která podporuje mnoho šifrovacích algoritmů, jako AES, Blowfish, Camellia a další. Šifrování AES patří mezi nejnovější technologie a je považována za nejlepší, protože nemá známé bezpečnostní slabiny [16]. OpenVPN funguje na operačních platformách Windows, Linux, Android a iOS. Navíc v routeru Turris, který byl zakoupen pro firmu je doplňující instalační balíček přímo pro OpenVPN.

3.2.3 Založení serveru

Po přihlášení do administrace a nastavení routeru v nabídce *Updater* bylo označeno nainstalování OpenVPN balíčku. Do nabídky routeru potom přibude položka OpenVPN.

Po rozkliknutí této položky se nám objeví instrukce pro nastavení OpenVPN serveru.

3.2.4 Vytvoření certifikátu

Jako první je nutné vytvořit certifikační autoritu. Na základě ní lze generovat klientské certifikáty. Certifikát je soubor, díky kterému se později budeme moc vzdáleně připojit. Každý potenciální uživatel musí certifikát mít.

Pro vygenerování certifikátu byla použita utilita „gen“, která byla nainstalována společně s balíčkem OpenVPN instalovaným z repositáře Turris. Jedna z možností, jak se dostat ke správě certifikátů, byla přes příkazový řádek pomocí SSH. Následující příkazy byly použity pro vygenerování certifikátů:

Příkaz pro vygenerování certifikační autority:

/usr/share/nuci/ca/gen new_ca openvpn

Příkaz pro vygenerování certifikátu klienta:

/ush/share/nuci/ca/gen switch openvpn gen_client "jmeno"

3.2.5 Konfigurace OpenVPN

Konfigurace OpenVPN je možná dvěma způsoby, buď přes grafické rozhraní, které umožňuje pouze základní konfiguraci, nebo je zde také možnost nastavení přes příkazový řádek (Obr. 3.9). Konfigurace musí probíhat pouze jen přes jedno z uvedených, navzájem se totiž ruší. Pokud bych tedy VPN nastavoval přes rozhraní FORIS a následně upravil něco přes příkazový řádek, první nastavení přes FORIS se mi resetuje a bude neaktivní. Samozřejmostí je potom zadání vlastní IP adresy VPN serveru.

```
root@turris:/etc/config# cat openvpn

config openvpn 'server_turris'
        option enabled '1'
        option port '1194'
        option proto 'udp'
        option dev 'tun_turris'
        option ca '/etc/ssl/ca/openvpn/ca.crt'
        option crl_verify '/etc/ssl/ca/openvpn/ca.crl'
        option cert '/etc/ssl/ca/openvpn/01.crt'
        option key '/etc/ssl/ca/openvpn/01.key'
        option dh '/etc/dhparam/dh-default.pem'
        option server '10.111.111.0 255.255.255.0'
        option ifconfig_pool_persist '/tmp/ipp.txt'
        option duplicate_cn '0'
        option keepalive '10 120'
        option comp_lzo 'yes'
        option persist_key '1'
        option persist_tun '1'
        option status '/tmp/openvpn-status.log'
        option verb '3'
        option mute '20'
        list push 'route 192.168.2.0 255.255.255.0'
```

Obrázek 3.9 *Konfigurace OpenVPN*

3.2.6 Nastavení klientů

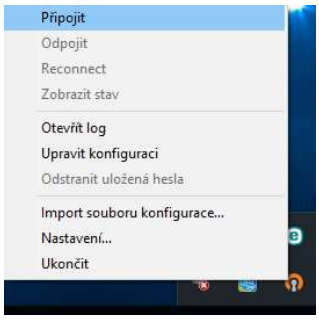
Je třeba také mít možnost vytvořit a zrušit přístup klientů do VPN sítě. Pro každého klienta se vytváří vlastní certifikát, který si nahraje do svého zařízení a pomocí něj se připojuje vzdáleně k síti. Dva uživatelé nemohou mít stejný certifikát, protože by docházelo ke kolizím a připojení by nebylo možné. Zvolí se název certifikátu a vytvoří se konfigurační soubor, který je následně možné stáhnout (a poskytnout danému zaměstnanci), anebo zrušit přístup již vytvořeného certifikátu.

3.2.7 Návod na instalaci OpenVPN klienta na různé platformy

3.2.8 Windows

1. Jako první je nutné stáhnout z oficiálních stránek OpenVPN klienta.
2. Stáhnutý soubor nainstalovat.
3. Je třeba mít od správce VPN serveru, na který se budete chtít připojovat, poskytnutý konfigurační soubor, který připojení umožní.
4. Pokud soubor již vlastníte, je třeba otevřít cílovou konfigurační složku, kde se musí umístit. Složka je umístěna podle toho, kde je OpenVPN nainstalováno. Nejčastěji tak bývá: Tento počítač - Místní disk (C:) – Program Files (x86) – OpenVPN. Zde je potřeba otevřít složku config a do ní přemístit konfigurační soubor.

5. Teď už jen stačí dvojklikem spustit OpenVPN program. S největší pravděpodobností se nic nezobrazí, to je však správně. Program běží na pozadí a lze jej najít v liště v pravo dole mezi skrytými ikonami.
6. Najetím myší na ikonu v dolní liště a pravým tlačítkem myši se rozbalí nabídka (Obr. 3.10). Zde je třeba kliknout na tlačítko připojit. Objeví se dialogové okno s logy a informacemi a poté by mělo vyskočit oznámení o úspěšném připojení.



Obrázek 3.10 *Připojení k OpenVPN*

7. Nyní je připojení přes OpenVPN do soukromé sítě funkční.

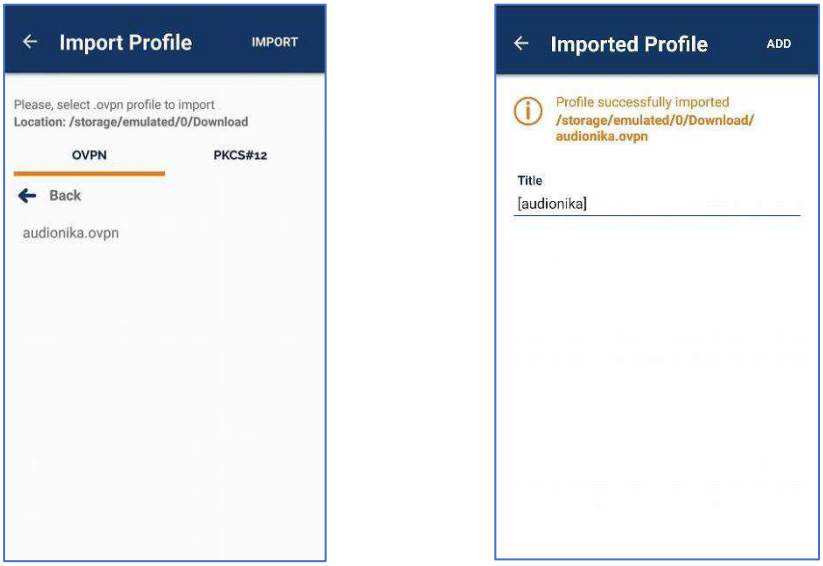
3.2.9 **Android**

1. Z obchodu Google Play je potřeba si stáhnout a nainstalovat aplikaci OpenVPN Connect – Fast & Safe SSL VPN Client (Obr. 3.11).
2. Je třeba mít v mobilu již nachystaný konfigurační soubor s příponou .ovpn, který vám poskytne správce VPN serveru, ke kterému se připojujete.
3. Po zapnutí aplikace se vybere třetí možnost v nabídce, a to je OVPN Profile

Obrázek 3.11 *Úvodní strana aplikace OpenVPN*

4. Pokud vyskočí požadavek k povolení přístupu aplikace k úložišti v telefonu, dáme povolit.
5. Aplikace si poté sama najde soubor s příponou .ovpn, pokud je v telefonu uložen. Zde stačí kliknout na tento soubor a dát *Import* nahoře v pravém rohu (Obr. 3.12).

6. V dalším okně se ukáže upozornění, zda byl soubor úspěšně importován a pokračuje se opět v horní pravém rohu tlačítkem add (Obr. 3.12).



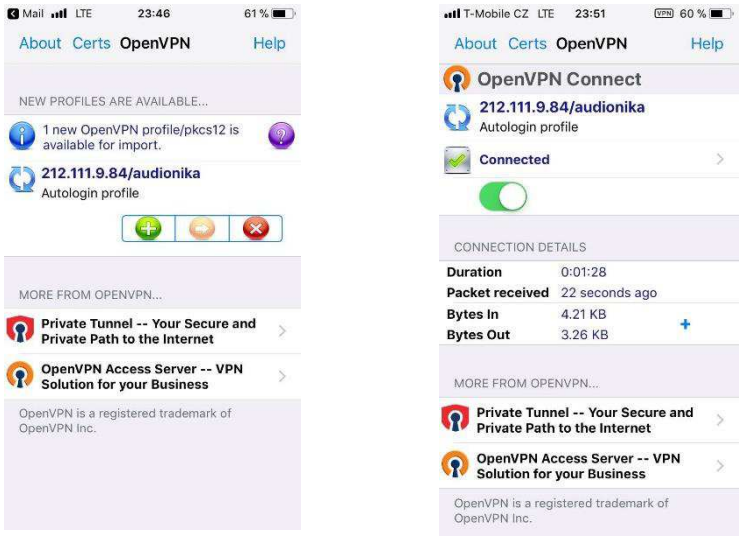
Obrázek 3.12 *Výběr a import konfiguračního souboru*

7. Po přidání profilu už stačí jen kliknout na VPN síť v nabídce a automaticky se provede připojení.

3.2.10 **iOS**

1. Z App Storu stáhněte a nainstalujte aplikaci OpenVPN Connect – Fast & Safe SSL VPN Client.
2. Konfigurační soubor poskytnutý poskytovatelem VPN serveru, ke kterému se budete moci připojit je třeba zaslat e-mailovou zprávou a otevřít v iPhone aplikaci Mail.
3. Po otevření e-mailu klikněte na přiložený soubor a zvolte možnost *Zkopírovat do:* OpenVPN
4. Stiskněte ikonu pro přidání VPN profilu (Obr. 3.13).
5. Vyskočí upozornění, které říká, že použitím OpenVPN může být veškerá aktivita na iPhonu filtrována nebo monitorována. Tuhle možnost povolte.

6. Aplikace se přesměruje na hlavní menu, kde se už stačí posunutím malého virtuálního kolečka připojit k VPN síti (Obr. 3.13).



Obrázek 3.13 *Přidání profilu OpenVPN a připojení k síti*

3.2.11 **Vytvoření vlastního instalačního souboru**

Součástí zadání bylo při zavedení VPN sítě vytvořit jednoduchou konfiguraci a instalaci a umožnit se tak připojit co nejjednodušeji pro nezkušené uživatele. Pro operační systém Windows jsem se tedy rozhodl udělat instalační balíček, který stačí pouze nainstalovat a vše už bude nastavené.

Jako první bylo třeba vygenerovat konfigurační soubory pro všechny zaměstnance a pro každého vytvořit tím pádem individuální instalační balíček. K možnému vytvoření instalačního balíčku je třeba lepší OpenVPN GUI Client který umožňuje provoz bez administerských práv a jsou k dispozici veškeré zdrojové a konfigurační soubory. Tento klient je funkční pouze pro Windows Vista a vyšší. Zároveň je potřeba skriptovací software NSIS, který umožňuje zabalit všechny zdrojové soubory do jednoho.

Napřed je třeba vložit konfigurační soubor do instalační složky. Každý klient bude mít tento soubor jiný a unikátní pouze pro jedno zařízení. Potom bylo nutné najít zdrojový soubor s názvem openvpn.nsi. Ten byl otevřen v textovém editoru a ve zdrojovém kódu byla změněna přístupová cesta ke konfiguračnímu souboru, aby se při instalaci rovnou také nainstalovala již požadovaná VPN síť (Obr. 3.14).

```
File "${BIN}\openvpn-gui.exe"

SetOutPath "$INSTDIR\config"
File "${HOME}\config\audionika.ovpn"

CreateDirectory "$INSTDIR\log"
CreateDirectory "$INSTDIR\config"
```

Obrázek 3.14 *Část kódu pro přiřazení konfiguračního souboru*

Po uložení stačilo kliknout pravým tlačítkem myši na tentýž soubor a vybrat možnost Compile NSIS Script. Je velmi důležité, aby všechny soubory byly ve stejném adresáři. Jinak nebude možné soubory zkompilovat do jednoho.

Po zkompilování se vytvoří jediný soubor, který stačí nahrát do příslušného PC s Windows (Vista +) a nainstalovat. Po nainstalování se může klient okamžitě připojit, aniž by cokoliv musel nastavovat.

3.2.12 **Nastavení pravidel v souvislosti s GDPR**

Kvůli zabezpečení se se pro VPN certifikáty využívá kryptografický algoritmus RSA s 4096 bitovým klíčem. K podepisování jednotlivých zpráv se používá hashovací algoritmus SHA256.

Pro ještě bezpečnější připojení k vytvořeným unikátním certifikátům pro každého zaměstnance bude ještě přidáno autentizační jméno a heslo, bude tedy nutné dvojité ověření. Zaměstnanec bude potřebovat certifikát určený přímo pro něj a zároveň přístupové údaje.

Pro vytvoření hesla pro daný certifikát je potřeba se připojit přes SSH k routeru a najít vygenerované certifikáty. Cesta k certifikátu je */etc/ssl/ca/openvpn*. V tomhle adresáři se vybere certifikát, který chci navíc zabezpečit a pomocí následujících příkazů vytvořím šifrování a heslo:

/etc/ssl/ca/openvpn cp 04.key 04.key~

/etc/ssl/ca/openvpn openssl rsa - aes256 -in 04.key -out 04.encrypted.key

/etc/ssl/ca/openvpn rm 04.key

/etc/ssl/ca/openvpn mv 04.encrypted.key 04.key

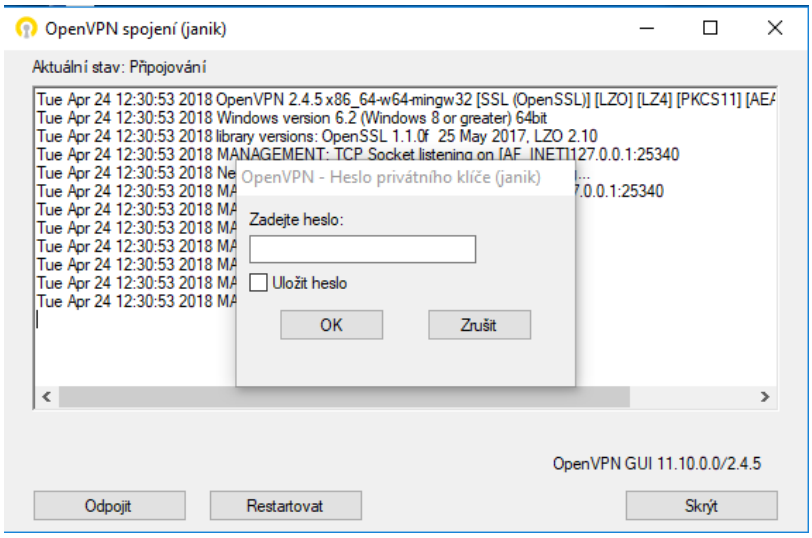
Zašifrované soubory *.key* a *.crt* bylo potřeba zkopírovat z paměti routeru na místní disk, aby mohly být upraveny a přidány do konfiguračního souboru k VPN. K přenosu souborů přes SSH byla využita utilita *scp*. V této utilitě běží protokol označovaný jako *SCP* (secure copy). *SCP* je prostředek bezpečného přenosu souborů mezi místním a vzdáleným hostitelem nebo mezi dvěma vzdálenými hostiteli a je založen právě na protokolu SSH. Poté už pomocí příkazového řádku ve Windows byla utilita spuštěna, připojilo se přes SSH k routeru a po zadání hesla a cesty k souborům se stáhnuly požadované soubory na místní disk (Obr. 3.15).

```
                    pscp.exe root@10.111.111.1:/etc/ssl/ca/openvpn/04.crt C:/
root@10.111.111.1's password:
04.crt                    | 6 kB |   6.7 kB/s | ETA: 00:00:00 | 100%

                    pscp.exe root@10.111.111.1:/etc/ssl/ca/openvpn/04.key C:/
root@10.111.111.1's password:
04.key                    | 3 kB |   3.2 kB/s | ETA: 00:00:00 | 100%
```

Obrázek 3.15 *Přenos souborů pomocí protokolu SCP*

Po vytvoření konfiguračního souboru *.ovpn* byl do souboru nakopírován obsah klíče a certifikátu, které byly v přechozím kroku upraveny. Při připojení k VPN je nyní vyžadováno heslo (Obr. 3.16).



Obrázek 3.16 *Autentizace pomocí privátního klíče*

3.3 Privátní cloudové úložiště s automatickým zálohováním dat

Aktuálně se pro zálohování dat používá externí disk, což je neefektivní, pokud bychom chtěli zálohovat data globálně a přistupovat k nim i vzdáleně. Zadáním bylo vybrat v poměru cena/výkon NAS úložiště, které by tento problém vyřešilo.

Parametry, podle kterých bylo vybráno:

- Počet připojených disků a jejich velikost
  - Velikost je důležitá. Pro zálohování jsem vybral dva 1TB HDD disky
- Rychlost čtení/zápisu zálohovaných dat
- Jaké RAID (Redundant Array of Independent Disks) podporuje, které slouží k zabezpečení dat proti selhání pevného disku.
  - Disky budou v RAID 1 (zrcadlení). To znamená, že obsah se současně zaznamenává na dva disky. V případě výpadku jednoho disku se pracuje s kopií, která je ihned k dispozici. Pokud tedy jeden harddisk odejde, všechna data budou dále k dispozici.
- Jaké platformy podporuje
  - Požaduje se, aby NAS podporovalo nejen Windows, na kterém běží všechny firemní počítače, ale také Android a iOS pro zálohování z mobilních zařízení.
- Jednoduché uživatelské rozhraní
  - Nastavení NAS serveru musí být co nejjednodušší vzhledem k tomu, že správců serveru bude později více.

Ve finálním výběru mezi několika NAS servery (QNAP TS-228, 228A, Synology) bylo rozhodnuto pro Synology DS218j (Obr. 3.17). Tento multimediální NAS má rychlost čtení 113 MB/s a rychlost zápisu 112 MB/s. V uvedeném parametru byl jednoznačně nejlepší. Server je dostupný z platforem Windows, Linux, Android a iOS. Jeho prostředí je jednoduché a přehledné. Zmíněný server má kapacitu úložiště až 24 TB, v našem případě tedy 2x 12 TB. Tuto kapacitu nebudeme ani zdaleka využívat, proto zatím stačí dva 2TB disky pro zálohování. Kapacitu lze kdykoliv rozšířit. K serveru můžeme připojit USB 3.0 a hlavně RJ-45 1Gbitový LAN kabel, přes který bude připojeno NAS k routeru. [17]

K NAS bude přístup pouze z interní sítě anebo díky možnosti vzdáleného přístupu přes VPN.

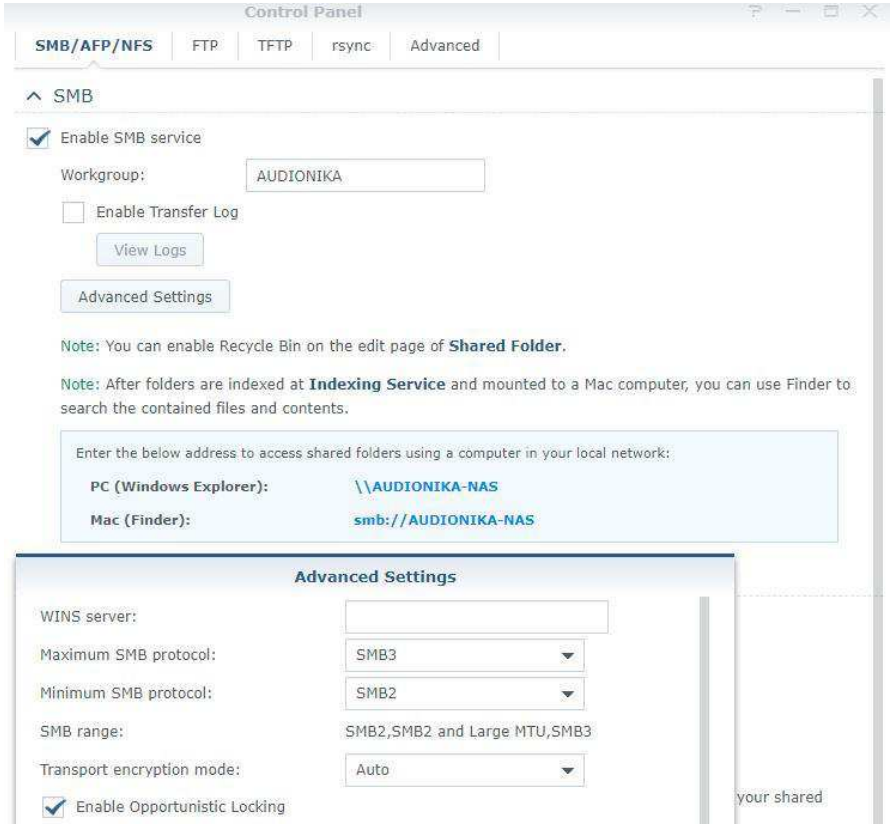
Obrázek 3.17 *Synology NAS [18]*

3.3.1 Nastavení NAS pro sdílení dat mezi zaměstnanci

Ověřování přístupu je nastaveno pro každého zaměstnance pomocí uživatelského jména a hesla. Ty byly nastaveny pomocí webového rozhraní v Synology NAS zařízení. Hesla byla již zaměstnancům přidělena a byla použita i pro přihlášení k NAS úložišti.

Pro celou firmu byla nastavena jedna sdílená globální složka AudioNIKA o velikosti objemu dat 10Gb. Tato složka bude společná pro všechny zaměstnance. Nastavení jedné složky bylo vytvořeno pro firmu jako pro skupinu, kde jsou nastavena přístupová práva skupinově a pro všechny uživatele stejně. Nebylo třeba nastavovat tyto údaje pro každého zvlášť. Pro každého zaměstnance byla jednotně vytvořena jejich soukromá složka zálohování dat. Každý uživatel má nastavenou svou privátní složku na zálohu o objemu 100 GB dat.

Rozhraní Synology umožňuje zálohování privátní složky, která je zpřístupněná přes protokol SMB. Procházení této složky je potom možné ve službě Synology NAS pomocí průzkumníka nebo připojením sdílené složky jako síťové jednotky. Synology NAS je nastaveno na minimální verzi SMB 2 a maximální SMB 3 (Obr. 3.18). Protokol SMB 3 se liší od nižší verze podporou pro Windows 8 a vyšší. Jedná se také o vylepšenou verzi protokolu SMB 2. SMB3 podporuje přenos šifrování souborů založený na AES (Advanced Encryption Standard), čímž zlepšuje zabezpečení přenosu souborů peer-to-peer rozhraní.



Obrázek 3.18 *Nastavení sdílené složky pomocí SMB protokolu*

3.3.2 Automatické zálohování zvolených adresářů z firemních zařízení

K zálohování se využívá aplikace Cloud Station, která slouží k jednoduché synchronizaci souborů na zařízení Synology NAS s ostatními zařízeními. Tyto zařízení musí disponovat utilitou DScloud, která pracuje právě pod záštitou Synology a funguje pouze pro jejich uživatele. Kromě Windows ji lze použít i pro ostatní platformy, jako jsou zařízení se systémem Android nebo iOS. Po nainstalování této aplikace jdou jednoduše vybrat složky, které se budou automaticky zálohovat.

Pro automatické zálohování souborů se již využíval placený nástroj Bvckup, kde pro začátečníky stačí vyplnit dvě pole – co zálohovat a kam zálohovat. Bvckup byl využíván pro zálohování dat na externí disk. Nastavení jsem tedy přesměroval na ukládání dat na NAS a na zálohování v noční dobu nebo při změně obsahu určitých složek. Záloha se bude provádět každých šest hodin a budou zachovány i zálohy již smazaných souborů a složek. NAS je dostupná i přes webové rozhraní v lokální síti. Na portu 5000 běží webová aplikace, přes kterou je možné úložiště spravovat. Druhá možnost je připojení k úložišti přes konzoli.

3.3.3 Dostupnost cloudových služeb z interní sítě a přes VPN

Synology NAS je třeba umístit do sítě tak, aby na něj byl přístup jak z interní sítě, tak přes VPN. Nicméně pro připojené uživatele přes VPN je důležité, aby byla viditelná pouze NAS a nebyl tak přístup k interní síti firmy. Z tohoto důvodu se rozhodlo pro rozdělení sítě do různých VLAN (*lan, lan2*).

Znamená to, že část portů na routeru Turris Omnia bude vyčleněno pro samostatnou firemní síť, která bude mít vlastní pravidla a především bude oddělena od druhé části sítě, ke které bude připojen Synology NAS a VPN. NAS bude umístěno do sítě *lan2*, která bude působit jako demilitarizovaná zóna, aby v případě kompromitace nemohl útočník zaútočit i na další počítače ve firemní síti.

Router Turris disponuje třemi síťovými rozhraními. Jedná se o rozhraní *eth0*, *eth1* a *eth2*. Rozhraní *eth1* je propojeno přímo s konektorem WAN a rozhraní *eth0* a *eth2* jsou připojena do switch-chipu k fyzickým portům 5 a 6. Switch-chip dále zajišťuje propojení s Porty 0 až 4, kterým jsou přiřazeny již standardní RJ-45 porty LAN 0 až LAN 4.

Pomocí SSH přístupu bylo docíleno konfigurace rozhraní firewallu a routeru tak, aby splňovali vymezené požadavky na síť. SSH přístup byl zvolen zejména proto, protože některé parametry nelze přes webové rozhraní konfigurovat.

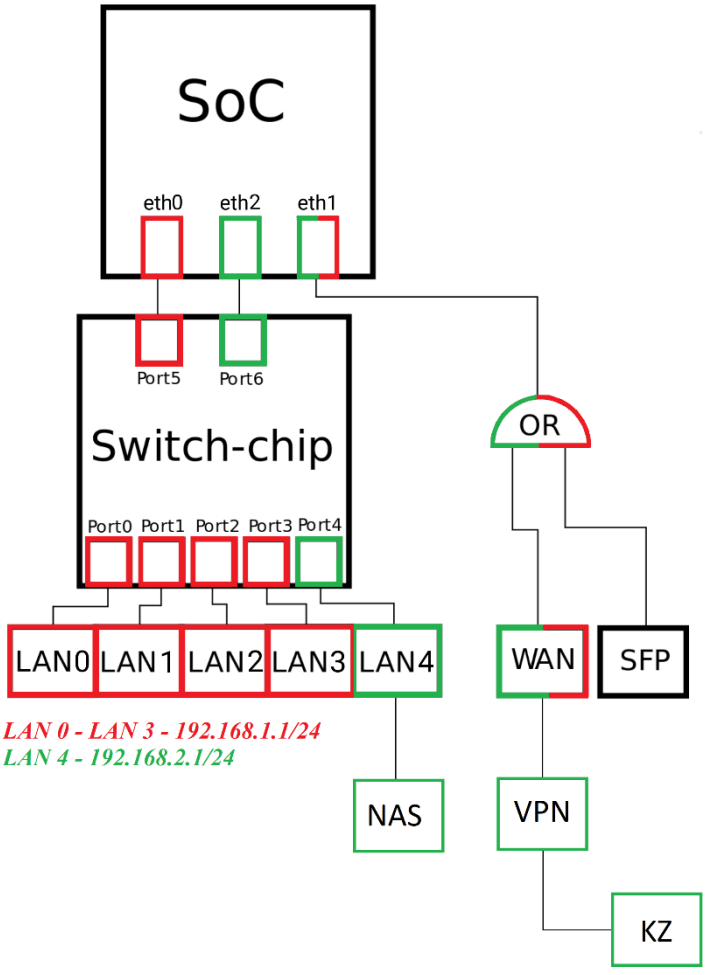
Pro připojení k routeru pomocí SSH jsem použil nástroj PuTTy, který byl shledán jako nejpřívětivější a nejjednodušší SSH klient pro platformu Windows.

Po připojení k routeru se bylo třeba dostat ke konfiguračním souborům pro síť, firewall a VPN. Interní LAN síti *lan2* byla přidělena IP adresa 192.168.2.1/24 (Obr. 3.19).

```
config interface 'lan2'
        option proto 'static'
        option netmask '255.255.255.0'
        option ip6assign '64'
        option _orig_ifname 'eth0.2'
        option _orig_bridge 'false'
        option ifname 'eth2'
        option ipaddr '192.168.2.1'
```

Obrázek 3.19 *Vytvoření sítě "lan2"*

Znázornění propojení a vytvoření dvou *lanů* bylo zakresleno do schématu, viz. Obr. 3.20.



Obrázek 3.20 *Hardwarový návrh a propojení jednotlivých rozhraní, resp. portů*

V konfiguračním souboru firewallu bylo nutné přidat novou zónu *lan2* a *vpn_turris*, které musely být nastaveny tak, aby byl přístup ke každé z nich povolen jen ze stanovených míst. Dále bylo potřeba nastavit tzv. Forwarding, který jednotlivé zóny propojuje (Obr. 3.21). V samotné definici zóny jsou nastavena pravidla pro vstup/výstup a přeposílání z a do zóny.

```
config zone 'lan2'
        option input 'ACCEPT'
        option output 'ACCEPT'
        option name 'lan2'
        option forward 'ACCEPT'
        option network 'lan2'

config zone 'vpn_turris'
        option name 'vpn_turris'
        option input 'ACCEPT'
        option output 'ACCEPT'
        option forward 'REJECT'
        option network 'vpn_turris'
```

```
config forwarding
        option dest 'wan'
        option src 'lan'

config forwarding
        option dest 'lan'
        option src 'lan2'

config forwarding
        option dest 'wan'
        option src 'lan2'

config forwarding
        option dest 'lan2'
        option src 'lan'

config forwarding
        option dest 'lan2'
        option src 'vpn_turris'
```

Obrázek 3.21 *Nastavení zón a jejich propojení*

3.3.4 Nastavení pravidel v souvislosti s GDPR

Synology NAS využívá šifrování na vysoké úrovni – šifrování AES (Advanced Encryption Standard). Přenos dat přes internet lze rovněž šifrovat, takže je bezpečné používat i služby jako File Station, FTP a další.

Dále je k dispozici dvoustupňové ověřování, což znamená, že při přihlášení do systému Synology NAS bude třeba ještě zadat další jednorázový ověřovací kód. Nepovolaní uživatelé by neměli mít přístup k datům bez použití dotyčného zařízení.

4 Teoretické a praktické znalosti a dovednosti

4.1 Uplatnění znalostí a dovedností získané studiem

Při absolvování odborné praxe byly využity znalosti, které jsem nabyl během studia na Vysoké škole báňské – Technické univerzitě Ostrava.

Mezi nejdůležitější předměty, které mi pomohly při plnění úkolů praxe, byl Přenos dat, díky kterému jsem už lépe rozuměl protokolu SMB, příkazovému řádku, práci se soubory, nebo firewallu.

Díky předmětu Telekomunikační sítě jsem mohl využít vědomosti ohledně Wi-Fi sítí a maximalizovat tak pokrytí a stabilitu firemní sítě.

Mnoho znalostí ohledně zdokonalení na lepší a rychlejší síť jsem také čerpal z předmětu Přístupové sítě, který mě vedl k získání většího přehledu v oblasti sítí.

4.2 Scházející teoretické a praktické znalosti

V průběhu absolvování odborné praxe mi scházely podrobnější znalosti při řešení jednotlivých problémů ve firmě. Například při vytváření VPN jsem neměl dostatečné znalosti příkazového řádku a konfigurace přes SSH. Nabytí těchto zkušeností beru jako velice přínosné.

Musel jsem se také velmi dobře seznámit s novým routerem a jeho dokumentací, díky níž jsem potom mohl realizovat autentizaci pomocí hesla i certifikátu, a hlavně vytvořit druhou síť, která umožňuje vzdálený přístup z VPN k privátnímu cloudu, avšak nikoli do ostatních zařízení ve firemní síti.

5 Dosažené výsledky a celkové hodnocení odborné praxe

5.1 Dosažené výsledky

Všechny výše uvedené úkoly jsem realizoval, implementoval a úspěšně dokončil.

V prvním úkolu jsem provedl vylepšení síťové infrastruktury, která zahrnuje zrychlení přístupu ke sdíleným zdrojům, navýšení stability a dostupnosti drátového i bezdrátového spojení, zabezpečení sítě a umožnění přístupu k internetu návštěvníkům firmy bez možnosti vstupu do interní sítě.

V druhém úkolu bylo nastaveno VPN připojení, vytvořil se server a návody pro připojení k operačním platformám, jako jsou Windows, iOS či Android. Zároveň byl vytvořen instalační balíček, díky kterému je velmi jednoduchá instalace i pro méně zkušené uživatele/zaměstnance. Z tohoto bodu bylo časově nejnáročnější vytvoření dvojí autentizace pomocí certifikátu a pomocí hesla přes příkazový řádek.

V posledním bodě jsem vybral vhodné cloudové úložiště, zapojil ho do interní sítě, nakonfiguroval a nastavil privátní složky pro každého zaměstnance s určitou kvótou na objem dat. Nastavil jsem automatické zálohování pomocí protokolu SMB z místních zařízení, a především jsem umožnil dostupnost těchto služeb jak z interní sítě, tak přes VPN. Tato úloha byla pro mne nejsložitější z celé praxe, protože jsem se musel podrobně naučit konfiguraci routeru a celého principu, jak je síť sestavena. Vytvoření podsítě mi dělalo původně problém a zabralo mnoho času, než jsem dokázal uvést vše do požadovaného stavu tak, aby cloudové úložiště bylo přístupné z obou sítí, ale zároveň, aby se zařízení připojené z odlišných sítí navzájem neviděly.

Nad rámec praxe jsem se také podílel na menších úkolech, které souvisely například s vylepšením firemních softwarů, školením zákazníků, či servisem audiologických přístrojů, sluchových implantátů a sluchadel.

5.2 Časová náročnost úkolů

Zadaný úkol	**Počet dní**
Vylepšení sítě	6
Rozdělení sítě a zabezpečení	4
Dokumentace konfigurace	3
GDPR	4
VPN	10
Vytvoření dvojí autentizace	4
Cloudové úložiště	7
Dostupnost NAS přes VPN a interní sítě	12
Technická podpora	3
Ostatní úkoly	6

Závěr

Absolvování odborné praxe ve firmě AudioNIKA s.r.o. mi přineslo spousty užitečných znalostí a zkušeností, které budou využity jak pro správu podnikové sítě v této firmě, tak v dalších pracovních aktivitách.

Nabyl jsem znalosti ohledně počítačových sítí, jejich konfigurace a také nastavení jednotlivých zařízení, firewallu, zálohovacích zařízení či VPN serveru. V této práci je popsán upgrade síťové infrastruktury na rychlejší a spolehlivější síť, vytvoření práv s omezeními pro návštěvníky či pracovníky firmy a lepší stabilita a pokrytí Wi-Fi sítě.

Přínosem této práce bude také popis vybrání správného VPN poskytovatele, podrobný návod nastavení OpenVPN na jednotlivých platformách nebo jednoduchá instalace softwaru pro nezkušené uživatele pomocí instalačního balíčku. Podstatným bylo také vytvoření dvojího zabezpečení, které zabrání připojení se k firemní sítí přes VPN nepovolaným účastníkům. Zabezpečení tvoří unikátní certifikáty pro každého zaměstnance a také ověření pomocí hesla.

Práce obsahuje také návod na nastavení OpenVPN přes příkazovou řádku pro TurrisOS.

Prohloubil jsem si znalosti s Turris OS prostředím, lépe se seznámil se zabezpečenou komunikací pomocí protokolu SSH a práce s ním. Naučil jsem se konfigurovat router nejen pomocí uživatelského prostředí, ale také pomocí složitějších metod přes příkazový řádek.

Vytvoření cloudového úložiště bylo taktéž velkým přínosem pro firmu, díky čemuž si může kdokoliv povolaný zálohovat data na firemní úložiště a mít tak přístup k zálohovaným souborům jak z firemní, tak ze vzdálené sítě. To byl pro mě nejsložitější úkol, u kterého jsem musel vytvořit oddělenou síť a úložiště umístit do vlastní zóny.

Také jsem se seznámil s prací se sluchadly a dalšími přístroji, které jsou běžně používány v audiologii, v oboru, kterým se firma převážně zabývá.

Odbornou praxi hodnotím velmi pozitivně a jsem rád, že jsem jí absolvoval, protože díky několika praktickým úkolům jsem pomohl jak firmě AudioNIKA s.r.o., tak svému růstu v oboru.

Použitá literatura

[1] Turris Omnia 2 GB Wi-Fi - WiFi router | Alza.cz. *Alza.cz - největší obchod s počítači a elektronikou | Alza.cz* [online]. Dostupné z: https://www.alza.cz/turris-omnia-2gb-d4480217.htm

[2] SSH honeypot – HaaS [Project: Turris]. *302 Found* [online]. Dostupné z: https://doc.turris.cz/doc/cs/howto/ssh_honeypot

[3] HOWTO. OpenVPN - Open Source VPN [online]. Copyright © 2002 [cit. 24.04.2018]. Dostupné z: https://openvpn.net/index.php/open-source/documentation/howto.html

[4] Wifi Heat Map - Survey - Apps on Google Play. [online]. Copyright ©2018 Google [cit. 29.04.2018]. Dostupné z: https://play.google.com/store/apps/details?id=info.wifianalyzer.heatmap

[5] Wifi Analyzer - Apps on Google Play. [online]. Copyright ©2018 Google [cit. 29.04.2018]. Dostupné z: https://play.google.com/store/apps/details?id=com.farproc.wifi.analyzer

[6] KRACK Attacks: Breaking WPA2. *KRACK Attacks: Breaking WPA2* [online]. Dostupné z: https://www.krackattacks.com/

[7] NEZMAR, Luděk. GDPR: praktický průvodce implementací. Praha: Grada Publishing, 2017. ISBN 978-80-271-0668-4

[8] Správce osobních údajů | GDPR.cz. GDPR | Obecné nařízení o ochraně osobních údajů — prakticky [online]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/spravce-osobnich-udaju/

[9] The best VPN service 2018 | TechRadar. *TechRadar | The source for tech buying advice | TechRadar* [online]. Copyright © Tunnelbear [cit. 29.04.2018]. Dostupné z: https://www.techradar.com/vpn/best-vpn

[10] Turris forum. Turris forum [online]. Dostupné z: https://forum.turris.cz/

[11] Oficiálnídokumentace [Project: Turris]. 302 Found [online]. Dostupné z: https://doc.turris.cz/doc/cs/howto/start

[12] AudioNIKA . Vítejte na našich stránkách. AudioNIKA . Vítejte na našich stránkách [online]. Copyright © [cit. 24.04.2018]. Dostupné z: http://www.audionika.cz/

[13] [online]. Copyright ©B [cit. 24.04.2018]. Dostupné z: https://global.download.synology.com/download/Document/UserGuide/DSM/5.2/Syno_UsersGuide_NAServer_enu.pdf

[14] DPO dle GDPR | Znalec v oborech Kybernetika a Ekonomika. *Znalec v oborech Kybernetika a Ekonomika* [online]. Copyright © 2018 [cit. 25.04.2018]. Dostupné z: https://znalecict.cz/index.php/gdpr/dpo-dle-gdpr/

[15] OpenVPN - Open Source VPN. *OpenVPN - Open Source VPN* [online]. Copyright © 2002 [cit. 25.04.2018]. Dostupné z: https://openvpn.net/

[16] Srovnání VPN Protokolů: PPTP vs. L2TP vs. OpenVPN vs. SSTP vs. IKEv2 | vpnMentor. *vpnMentor | 2018 Recenze, Tipy a VPN Tutoriály* [online]. Copyright © 2018 vpnMentor [cit. 29.04.2018]. Dostupné z: https://cs.vpnmentor.com/blog/srovnani-vpn-protokolu-pptp-vs-l2tp-vs-openvpn-vs-sstp-vs-ikev2/

[17] Synology DiskStation DS218j Review | Trusted Reviews. *TrustedReviews - The Why Before You Buy* [online]. Copyright © Copyright Time Inc. [cit. 29.04.2018]. Dostupné z: http://www.trustedreviews.com/reviews/synology-diskstation-ds218j

[18] NAS - Armazenamento - PCDIGA. *Home - PCDIGA* [online]. Copyright © 2017 PCDIGA. Todos os Direitos Reservados. [cit. 29.04.2018]. Dostupné z: https://www.pcdiga.com/nas

[19] General Data Protection Regulation (GDPR) | EARCHIVACE. *Hlavní stránka | EARCHIVACE* [online]. Copyright © 2014 [cit. 29.04.2018]. Dostupné z: http://www.earchivace.cz/clanky/general-data-protection-regulation-gdpr/